



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO. &	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/630,256	07/31/2000	Christopher L. Hamlin	K35A0635	5608

26332 7590 03/29/2004

WESTERN DIGITAL CORP.
20511 LAKE FOREST DRIVE
C205 - INTELLECTUAL PROPERTY DEPARTMENT
LAKE FOREST, CA 92630

EXAMINER

ZIA, MOSSADEQ

ART UNIT PAPER NUMBER

2134

7

DATE MAILED: 03/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/630,256

Applicant(s)

HAMLIN, CHRISTOPHER L.

Examiner

Mossadeq Zia

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 July 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-31 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 July 2000 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>4.5</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 10-15, 17, 26-31 are rejected under **35 U.S.C. 102(b)** as anticipated by Patent No. 5677952 Blakley, III et al.

3. Regarding claims 1 and 15, Blakley shows a disk drive 2 comprising:

(a) a disk 4 for storing data, the disk 4 comprising a public area 6 for storing plaintext data and a pristine area 8 for storing encrypted data (Blakley, col. 6, line 67);

(b) a head 10 for reading the encrypted data from the pristine area 8 (it is the interpretation of this examiner that encrypted data is read from an area or disk sector where the data is stored. It is considered pristine because it cannot be read without password authorization, (Blakley, col. 6, line 4-5, 23-24) of the disk 4 (head is feature of a disk drive device, see definition sited from MS Computer Dictionary));

(c) a control system 12 for controlling access to the pristine area 8 of the disk 4 (disk controller, Blakley, fig. 3, label 35);

(d) authentication circuitry 14 for authenticating a request received from an external entity to access the pristine area 8 of the disk 4 and for enabling the control system 12 if the request is authenticated (operating system, Blakley, fig. 3, label 78, 80, col. 6, 23-24);

Art Unit: 2134

- (e) a secret drive key 16 (secret key, Blakley, col. 5, line 47); and
 - (f) decryption circuitry 18, responsive to the secret drive key 16, for decrypting the encrypted data stored in the pristine area 8 of the disk 4 to generate decrypted data (device driver, Blakley, col. 4, line 66-67, col. 5, line 1, fig. 3, label 76).
4. Regarding claim 10, Blakley shows the disk drive of claim 1 above, and further show the encrypted data comprises encrypted message data (Blakley, col. 10, line 18-19).
5. Regarding claim 11, Blakley shows the disk drive of claim 1 above, and further show the disk drive further comprises encryption circuitry for encrypting plaintext data into the encrypted data stored in the pristine area (Blakley, col. 5, line 27-28, col. 6, line 66).
6. Regarding claim 12, Blakley shows the disk drive of claim 1 above, and further show:
- (a) the disk further comprises embedded servo sectors comprising servo bursts (read/write, col. 5, line 26-28);
 - (b) the control system comprises a servo control system responsive to the embedded servo sectors (disk controller, Blakley, fig. 3, label 35); and
 - (c) the authentication circuitry enables the servo control system (operating system, Blakley, fig. 3, label 78, 80, col. 6, 23-24).
7. Regarding claim 13, Blakley shows the disk drive of claim 12, wherein:
- (a) the servo bursts are written to the disk in encrypted form (write, Blakley, col. 5, line 26-28, 39-40); and
 - (b) the authentication circuitry enables the servo control system to decrypt the servo bursts (read, Blakley, col. 5, line 26-28, col. 6, line 35-36).
8. Regarding claim 14, Blakley shows the disk drive of claim 13, and further show:

Art Unit: 2134

(a) the servo bursts are written to the disk with additive noise generated from a pseudo random sequence (it is this examiners understanding that this is an inherent behavior driven by the data stream written to disk via the disk drive mechanism, where in this case the data being written is effected by the encryption key);

(b) the pseudo random sequence is generated from a polynomial (pseudorandom generator, col. 8, line 40);

(c) the servo control system uses the polynomial to decrypt the servo bursts (read, Blakley, col. 5, line 26-28, col. 6, line 35-36); and

(d) the authentication circuitry provides the polynomial to the servo control system (password determines secret key, Blakley, col. 7, line 43-47).

9. Regarding claim 17, Blakley show a method of processing a request received by a disk drive from an external entity to access encrypted data stored in a pristine area of a disk, the method comprising the steps of:

(a) authenticating the request to access the pristine area and enabling access to the pristine area if the request is authenticated (Blakley, col. 6, line 21-24, 27-28);

(b) reading the encrypted data stored in the pristine area (Blakley, col. 7, line 15-20); and

(c) decrypting the encrypted data using a secret drive key within the disk drive to generate decrypted data (Blakley, col. 11, line 45-49).

10. Regarding claim 26, see reasoning for claim 10 above.

11. Regarding claim 27, see reasoning for claim 11 above.

Art Unit: 2134

12. Regarding claim 28, Blakley show method as recited in claim 17 above, and further show the disk comprises embedded servo sectors comprising servo bursts, the method further comprising the steps of

(a) servoing a head over the disk in response to the embedded servo sectors (disk controller, Blakley, fig. 3, label 35); and

(b) enabling servoing in the pristine area if the request is authenticated read, (Blakley, col. 5, line 26-28, col. 6, line 35-36).

13. Regarding claim 29, see reasoning in claim 13 above.

14. Regarding claim 30, see reasoning in claim 14 above.

15. Regarding claim 31, Blakley show a method of processing a request received by a disk drive from an external entity to access data stored on a disk, the disk comprising a public area for storing plaintext data and a pristine area for storing encrypted data, the method comprising the steps of:

(a) decrypting the encrypted data stored in the pristine area of the disk using a secret drive key within the disk drive to generate decrypted data (Blakley, col. 4, line 66-67, col. 5, line 1, fig. 3, label 76); and

(b) using the decrypted data to authenticate the request received from the external entity before allowing access to the disk (Blakley, fig. 3, label 78, 80, col. 6, 23-24).

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2134

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

17. Claims 9, 25 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5677952 Blakley, III et al. in view of Patent No. 5235641 Nozawa et al.

18. Regarding claim 9, Blakley shows the disk drive of claim 1 above, but fails to show wherein the encrypted data comprises encrypted key data for decrypting an encrypted message.

However Nozawa et al. teach by causing the cryptographic device on the upper rank apparatus side to perform complicated and high-degree encryption of the data key, the encrypted data key and ordinary data encrypted on the basis of the data key in the external storage device can be safely and easily stored in one and the same recording medium. (Nozawa, col. 9, line 38-43).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Blakley as per teaching of Nozawa et al. such that the data key and the data encrypted by the data key can be managed safely and easily (Nozawa, col. 9, line 44-45).

19. Regarding claim 25, Blakley shows the disk drive of claim 17 above, but fails to show wherein the encrypted data comprises encrypted key data for decrypting an encrypted message.

However Nozawa et al. teach by causing the cryptographic device on the upper rank apparatus side to perform complicated and high-degree encryption of the data key, the encrypted data key and ordinary data encrypted on the basis of the data key in the external storage device can be safely and easily stored in one and the same recording medium. (Nozawa, col. 9, line 38-43).

Art Unit: 2134

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Blakley as per teaching of Nozawa et al. such that the data key and the data encrypted by the data key can be managed safely and easily (Nozawa, col. 9, line 44-45).

20. Claims 2-8, 18-24 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5677952 Blakley, III et al. in view of Patent No. EP 816967 A2 Scott et al.

21. Regarding claim 2, Blakley shows the disk drive of claim 1 above, but fail to show the encrypted data comprises encrypted authentication data.

However, Scott et al. shows method of creating a secure file by receiving an indication that an entity desires to perform a file access operation on a file of the data processing system; obtaining a private key of the entity; receiving data of the file to be created; determining a checksum (authentication data) of the file; encrypting the checksum using the private key; and creating the file and an associated affidavit that includes the encrypted checksum (Scott, col. 2, line 30-36).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Blakley et al. as per teaching of Scott et al. to include the method to gain the advantage of an automatic and transparent method of checking and authenticating software and data in a computer system.

22. Regarding claim 3, Blakley shows disk drive of claim 2 above, and further show the authentication circuitry is responsive to the decrypted data (Blakley, col. 7, line 15-20).

23. Regarding claim 4, Blakley shows the disk drive of claim 2 above, and further show the encrypted authentication data comprises encrypted user authentication data (password, Blakley, col. 5, line 66-67).

Art Unit: 2134

24. Regarding claim 5, Blakley shows the disk drive of claim 2 above, and further show the encrypted authentication data comprises encrypted device authentication data for authenticating a device, the device comprising a unique device ID configured during manufacture of the device (Blakley, col. 11, line 45-49).

25. Regarding claim 6, Blakley shows the disk drive of claim 2 above, and further show the encrypted authentication data comprises encrypted information for implementing a challenge and response verification sequence device (queries, Blakley, col. 5, line 43-44).

26. Regarding claim 7, Blakley shows the disk drive of claim 2 above, and further show the encrypted authentication data comprises encrypted message authentication data (checksum, Scott, col. 2, line 34).

27. Regarding claim 8, Blakley shows the disk drive of claim 7 above, and further show the encrypted authentication data comprises encrypted key data (secret or private key) for generating a message authentication code (Blakley, col. 5, line 66-67, Scott, col. 7, line 23-24).

28. Regarding claim 18, Blakley shows the disk drive of claim 2 above, but fail to show the encrypted authentication data comprises encrypted message authentication data.

However, Scott et al. shows method of creating a secure file by receiving an indication that an entity desires to perform a file access operation on a file of the data processing system; obtaining a private key of the entity; receiving data of the file to be created; determining a checksum (message authentication data) of the file; encrypting the checksum using the private key; and creating the file and an associated affidavit that includes the encrypted checksum (Scott, col. 2, line 30-36).

Art Unit: 2134

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Blakley et al. as per teaching of Scott et al. to include the method to gain the advantage of an automatic and transparent method of checking and authenticating software and data in a computer system.

29. Regarding claim 19, Blakley and Scott show method as recited in claim 18 above, and further show wherein the step of authenticating is responsive to the decrypted data (Scott, col. 7, 29-30, Blakley, col. 6, line 32, 35-36).

30. Regarding claim 20, Blakley and Scott show method as recited in claim 18 above, and further show the encrypted authentication data comprises encrypted user authentication data (password, Blakley, col. 5, line 66-67).

31. Regarding claim 21, see reasoning for claim 5 above.

32. Regarding claim 22, see reasoning for claim 6 above.

33. Regarding claim 23, see reasoning for claim 7 above.

34. Regarding claim 24, see reasoning for claim 8 above.

35. Claims 16 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5677952 Blakley, III et al. in view of Patent No. 5915018 Aucsmith.

36. Regarding claim 16, Blakley shows a disk drive 2 comprising:

(a) a disk 4 for storing data, the disk 4 comprising a public area 6 for storing plaintext data and a pristine area 8 for storing encrypted data (see reasoning in claim 1, section a);

(b) a head 10 for reading the encrypted data from the pristine area 8 of the disk 4 (see reasoning in claim 1, section b);

(c) a control system 12 for controlling access to the pristine area 8 of the disk 4 (see reasoning in claim 1, section c);

(d) a secret drive key 16 (see reasoning in claim 1, section e); and

(e) decryption circuitry 18, responsive to the secret drive key, for decrypting the encrypted data stored in the pristine area 6 of the disk 4, wherein:

the disk 4 comprises a plurality of physical blocks accessed by the control system through physical block addresses (Blakley, col. 3, line 48-49);

a request received from an external entity during normal operation of the disk drive comprises a logical block address (index) which is mapped by the control system to a selected one of the physical block addresses (Blakley, col. 2, line 11-14); but fail to show

the pristine area comprises at least one physical block written with at least part of the encrypted data during manufacturing of the disk drive and not externally accessible through a logical block address during normal operation of the disk drive.

However, Aucsmith shows a system for Digital Video Disc (DVD) copy protection scheme, where a DVD having compressed, encrypted content written on a first portion of the disc, and the content encryption key, itself encrypted with a second key and written out of band on a second portion of the disc is used to provide content, key, and control information to a DVD drive (inferred that data was encrypted during manufacturing of the disc, col. 2, line 50-54, the term out of band refers to data written on a DVD in such a way that it cannot be addressed by normal program logic thus not externally accessible, col. 3, line 64-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Blakley as per teaching of Aucsmith to have secure distribution and

Art Unit: 2134

management of cryptographic keys for use in a DVD copy protection scheme (Aucsmith, col. 2, line 46-48).

Conclusion


37. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia
Examiner
Art Unit 2134

mz
3/17/04


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100